ManageEngine
Log360

DATASHEET

Threat detection and response with Log360

Your IT infrastructure is large and complex, and often involves various connected endpoints. Despite your best efforts to secure your network, threat actors like malware and malicious insiders can lurk dormant on infected machines for days or even weeks after slipping past your security systems. Threat detection is the process of thoroughly analyzing your network to identify threat actors that have slipped past your defense systems which could potentially compromise your network.

Effective threat and attack detection should be an important part of any organization's cybersecurity strategy because responding to and recovering from an attack is largely dependent on early detection. Log360, a comprehensive security information and event management (SIEM) tool, helps you detect and respond to threats and attacks, and helps you overcome your IT security challenges.

Log360's threat detection capabilities

Listed below are some of Log360's threat detection capabilities.

- **Threat intelligence database**

Log360 is integrated with the world's most authoritative threat information sharing and analysis networks, like Webroot and AlienVault OTX, using STIX and TAXII protocols. It continuously correlates your connections with a blacklist of IPs and triggers alerts when there is a match, which is indicative of unsecure or malicious activity.

- **Threat Intelligence add-on for advanced threat analytics**

The advanced threat analytics feature gives valuable insights into the severity of threats using a reputation score for potentially malicious URLs, domains, and IP addresses. The reputation score is indicative of the potential degree of damage the malicious connection can do to your network.

- **Correlation to detect threats**

Identify attack patterns accurately with Log360's real-time correlation engine. The correlation engine discovers sequences of logs, coming from devices across your network, that indicate possible attacks, and quickly alerts you about the threat. Building strong event log correlation and analysis capabilities empowers you to start taking proactive steps against network attacks.

- **Machine-learning-powered UEBA to mitigate threats**

Using user entity and behavior analytics (UEBA) that employs machine-learning algorithms to accurately differentiate between a legit account's activity from a compromised one, and recognizing anomalies that indicate a threat or an attack.

Log360's threat response capabilities

- **Real-time event response system**

Log360 enables you to respond to critical security events promptly with its real-time event response system. It creates tickets from alerts and assigns them to the right administrator based on the device or device group that generated the alert.

- **Efficient alerting console**

Log360's alerting module helps security teams detect and mitigate security threats at an early stage. It can send you notifications on critical activities and changes happening in your network via email or SMS.

- **Automated incident workflows**

Log360's automated workflow management console allows you to mitigate security incidents in your network before they result in a breach by automating response workflows when alerts are triggered. You can create and manage common incident response steps such as disabling USB ports, shutting down systems, and changing firewall rules when security incidents are detected.

- **Intuitive reporting console**

Log360 provides you with an intuitive reporting console that delivers insightful reports and trend graphs which help you conduct effective investigation on events and in responding to anomalies effectively.

A use case of Log360's attack detection capability

Consider a scenario where John, a malicious insider, logs in after work hours and accesses sensitive company data. John then copies the multiple files that contain the sensitive data to his USB drive and logs out. Log360's UEBA immediately reports and alerts on both the unusual login activity and the malicious file export activity. With an automated workflow configured for disabling the user account when unusual logins are followed by file exports, you can detect John's data exfiltration attempt and immediately disable his account.

As soon as the admin is notified, they can take a quick glance at the trends in the abnormal login activity and unusual export pattern. They can investigate further by performing a quick forensic analysis with the search tool, accessing all the logs from John's activity. If the logs confirm suspicious activity, the admin can take further action.

Other highlights of Log360

- **Secure log archival**
  Its flexible archiving options enable you to archive logs automatically at custom intervals and store them in an encrypted form for as long as needed.

- **Forensic analysis with log search**
  Its powerful search engine helps you backtrack so you can pinpoint the security incident and extract crucial data to file an incident report.

- **Efficient compliance management**
  Its compliance management capabilities help organizations meet their varied auditing, security, and compliance needs.

- **Automatic discovery**
  It automatically discovers Windows and Linux/Unix devices, network devices, SQL servers, and IIS web servers in your network.

- **Easy deployment**
  Its quick and easy deployment lets you start analyzing logs in the form of graphs, charts, and other visual representations within minutes of installation.

Supported log sources

Log360 supports log analysis and parsing from over 750 log sources. The tool also includes a ustom log parser to analyze any human-readable log format. Some of the widely used log sources are mentioned below.

Applications
SQL and Oracle databases, IIS and Apache web servers, and more.

File servers
Windows, NetApp filers, EMC file servers, Synology NAS servers, Hitachi NAS servers, and file server clusters.

Network perimeter devices
Routers, switches, firewalls, IDS/IPS, and more.

Virtual platforms
Microsoft Hyper-V and VMware.

Cloud platforms
Azure, AWS, Salesforce, Office 365, and Exchange Online.

Linux/Unix servers and devices

Windows servers and workstations

System Requirements

Hardware requirements

Log360 on-premise deployment requires a dedicated server with the following hardware configuration.

Hardware	Minimum	Recommended
Processor	2.4 Ghz	3 Ghz
Core	Dual core	8 core
RAM	8 GB	16 GB
Disk space	60 GB	150 GB

Software requirements

ManageEngine Log360 supports the following Microsoft Windows operating system versions:

- Windows 2003
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 7
- Windows 8
- Windows 10
- Windows Server 2016
- Windows Server 2019

Supported browsers

ManageEngine Log360 requires one of the following browsers to be installed on the system to access the Log360 web client.

- Internet Explorer 9 and above
- Firefox 4 and above
- Chrome 10 and above
- Safari 5 and above

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

ManageEngine
Log360

$ Get Quote

Download